# Release Notes

MXtreme™ Mail Firewall 6.0
Update 3

Software Version: MXtreme 6.0 Update 3
Date: 6/30/2006

BorderWare Technologies
www.borderware.com

# Preface

These Release Notes describe the new features, enhancements, issues fixed, and any known issues for the MXtreme 6.0 Update 3 release, and contains the following sections:

- **What's New in Update 3** – Describes the new features and enhancements for this release.
- **Product Notes** – Describes any modifications or enhancements to existing features.
- **Issues Fixed In This Release** – Describes any previous issues that were fixed in this release.
- **Known Issues In This Release** – Describes any known issues with this release.
- **Dependencies** – Indicates any software dependencies and compatibility issues for this release.
- **Installation Notes** – Describes the installation procedure for installing or upgrading to this release.

⚠ *It is critical that the **Dependencies** and **Installation Notes** section be reviewed before installing this release.*

## Product Documentation

The MXtreme documentation set consists of the following documents:

| Document | Description |
|---|---|
| **Release Notes** | Provides up to date information on the product, including new features, improvements, issues fixed, and any known issues. If instructions in the ***Release Notes*** differ from the ***Installation Guide*** or ***User Guide***, use the instructions in the ***Release Notes***. |
| **Installation Guide** | Provides detailed information on how to install and provide the initial configuration for the MXtreme Mail Firewall. |
| **User Guide** | Provides detailed information on how to configure and administer the MXtreme Mail Firewall. |
| **MXtreme PostX Configuration Guide** | Describes how to configure MXtreme's integrated PostX encryption features. |

## Conventions

The following typographical conventions are used in this guide:

| Typeface or Symbol | Description | Example |
|---|---|---|
| *italic* | Screen name or data field names | *Activity Screen*, or *SMTP Port* |
| **bold** | Button names, Menu items, and Screen names | Select **Mail Delivery → Anti-Spam** on the menu and click the **Apply** button. |
| `courier font` | Text displayed on the screen and File and Directory names | `/backup/backup.gzip` |
| **`Bold courier`** | Text entered by the user | Enter: **`example.com`** |
| ℹ | Information that describes important features or instructions | Please see the following section for more details. |
| ⚠ | Information that alerts you to potential problems and issues | Use caution when enabling this feature. |

## Documentation Feedback

BorderWare welcomes any feedback or suggestions concerning the MXtreme documentation. Please send any comments, corrections, and suggestions for improvement to: `docfeedback@borderware.com`

## Technical Support

Contact your reseller or distributor for all technical support issues.

If you have purchased a technical support contract from your reseller, you are entitled to telephone support and other locally specified services, in addition to upgrades and patches as provided by BorderWare. BorderWare provides escalation and emergency support for reseller technical support personnel.

## Copyright Information

The contents of this document may refer to technologies that are under development and are subject to change without notice.

# What's New in Update 3

The following sections describe the new features in this release:

## PostX Message Encryption

This release adds integrated PostX message encryption allowing users to encrypt outbound messages directly from MXtreme without the need for a local encryption server or additional desktop software. Messages are secured until they are delivered and decrypted by the recipient of the message.

Integrated PostX encryption allows organizations to easily enforce company policies and compliancy rules with the secure delivery of encrypted messages without the need for the recipient to download or install any special software. PostX encryption uses the PostX Registered Envelope technology which creates an encrypted message for the recipient that can be read by opening the attachment in the message to provide the decrypted message.

PostX integration allows MXtreme to be configured to use the public PostX key server (`pxmail.com`) for services and key-exchange related activities, or a local PostX key server on the customer premises can be used.

This feature is configured via **Mail Delivery** → **PostX Encryption** on the menu.

Please see the ***MXtreme PostX Configuration Guide*** for more details on configuring this feature.

*PostX Encryption is a licensed option and requires a license key that can be obtained from BorderWare. A license key is also required for evaluations.*

## Threat Outbreak Control

The Threat Outbreak Control feature provides customers with zero-day protection against early virus outbreaks. For most virus attacks, the time from the moment the virus is released to the time a pattern file is available to protect against the virus can be several hours. During this period, mail recipients are vulnerable to potential threats.

MXtreme's Threat Outbreak Controls can detect and take action against early virus outbreaks to contain the virus threat. If a message is classified as containing a possible virus, the message can be quarantined, deleted, or the event can be logged. When an updated anti-virus pattern file is received, any quarantined files will be rescanned and non-viruses will be released. If a virus is detected with the new pattern file, the configured anti-virus action is performed on the message. If the hold period for a message in the quarantine expires and it has not been positively identified as a virus, the configured "release" action will be performed.

MXtreme will examine incoming "untrusted" messages and look for the following characteristics when deciding if the message indicates an early virus threat:

- The message is bulk (addressed to a large number of recipients) and contains an executable or common office document attachment (such as `.doc`). To detect the message as "Bulk", the Intercept *Bulk Analysis* feature must be enabled.

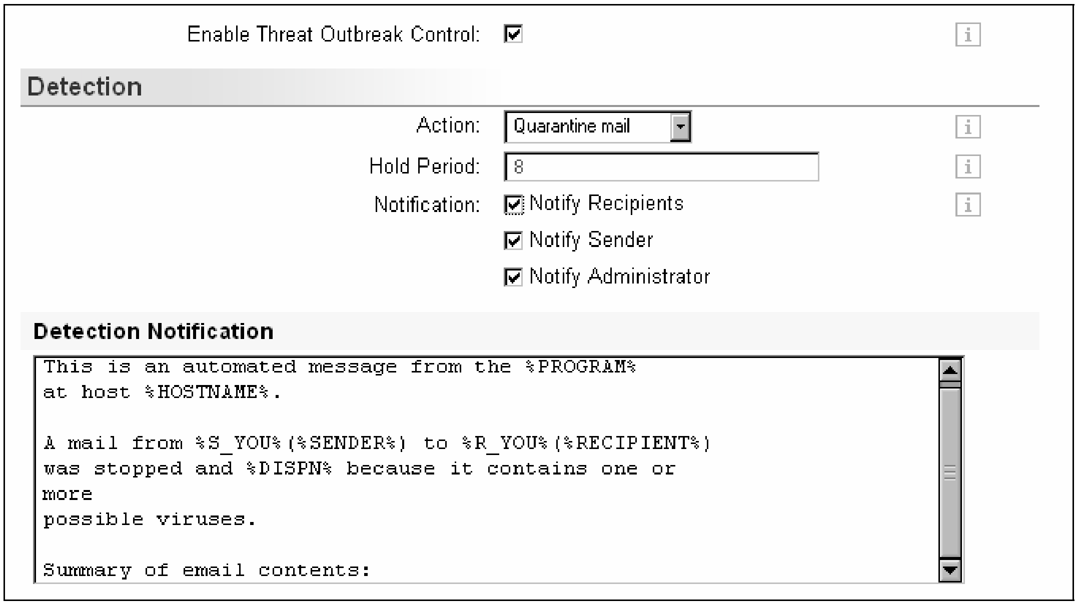
- The message originates from an IP address that has recently sent viruses and contains an executable or common office document attachment. To detect if the client has recently sent viruses, the *Mail Anomalies* feature and the "Recent virus from Client" option must be enabled.

- The message originates from an IP address with a poor *BorderWare Security Network (BSN)* reputation and contains an executable or common document attachment. To detect addresses with a poor reputation, the *BSN* feature must be enabled.

- The anti-virus scanner detects attachments that resemble a known virus or contain unknown viral code.

- The message was malformed, or was blocked by attachment control and the action was set to "Discard" or "Reject".

Select **Mail Delivery → Outbreak Control** on the menu to configure the Threat Outbreak Control feature.



Enable Threat Outbreak Control: ☑

Detection

Action: Quarantine mail

Hold Period: 8

Notification: ☑ Notify Recipients

☑ Notify Sender

☑ Notify Administrator

Detection Notification

```
This is an automated message from the %PROGRAM%
at host %HOSTNAME%.

A mail from %S_YOU%(%SENDER%) to %R_YOU%(%RECIPIENT%)
was stopped and %DISPN% because it contains one or
more
possible viruses.

Summary of email contents:
```

**Detection**
The following options take effect when Threat Outbreak Control is enabled:

- **Action –** Select the action to perform if a message is detected as having a possible virus:

  - **Just Log**: The message will be delivered and an entry added to the mail logs.
  - **Reject mail**: The message will be rejected with notification to the sender.
  - **Quarantine mail**: The message will be placed into the administrative quarantine area. These messages can be viewed and managed via **Status/Reporting → Quarantine** on the menu.
  - **Discard mail**: The message will be discarded without notification to the sender.

- **Hold Period –** Enter the time period (in hours) for which to hold the message in the administrative quarantine area. The default is 8 hours. It is recommended that enough time is configured to allow the opportunity for the files to be rescanned with updated anti-virus pattern files as they become available. If a quarantined message is rescanned and determined to have a virus, the configured anti-virus action will be performed, as set in **Mail Delivery → Anti-Virus**. If the hold period expires and the message has been determined not to be infected with a virus, the "Release" action will be performed.

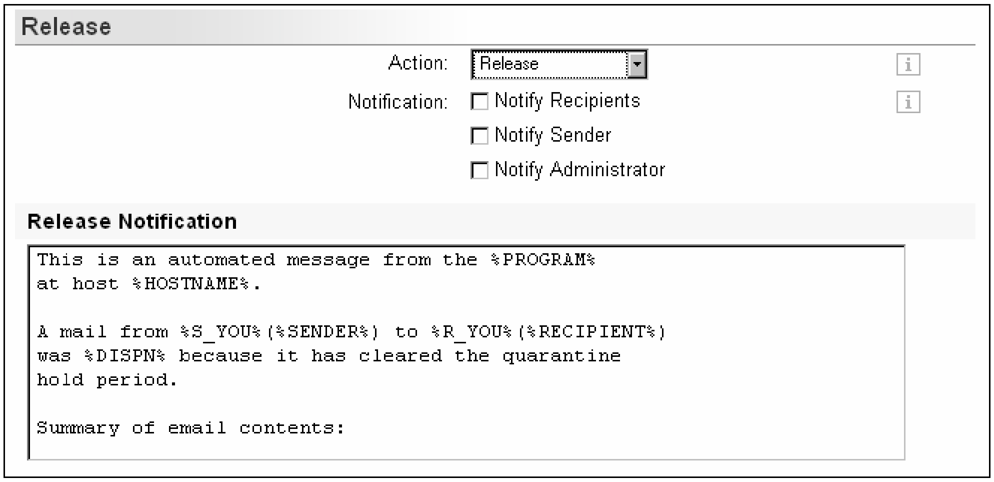
*If the Quarantine expiry period is set to a value less than the "Hold Period", the expiry period takes precedence and the held message will be expired.*

- **Notification –** Select the users who will receive a notification if a message is detected as having a possible virus. Options include the "Recipients", the "Sender", and the "Administrator".

- **Notification Message –** Enter the text for the automated notification message.

**Release**

The following options take effect for a quarantined message when its configured "Hold Period" has elapsed:



Release

Action: Release

Notification: □ Notify Recipients
□ Notify Sender
□ Notify Administrator

Release Notification

```
This is an automated message from the %PROGRAM%
at host %HOSTNAME%.

A mail from %S_YOU%(%SENDER%) to %R_YOU%(%RECIPIENT%)
was %DISPN% because it has cleared the quarantine
hold period.

Summary of email contents:
```

- **Action –** Select the action to perform if the "Hold Period" has elapsed for a quarantined message:

  - **Just Notify**: A message will be sent to notify the specified users that the "Hold Period" for a quarantined message has elapsed without it being classified as a virus.
  - **Release mail**: The message will be released from the quarantine and delivered to the original recipients. Notifications can also be enabled to notify users when the message is released.

- **Notification –** Select the users who will receive a notification if a message is released from the quarantine. Options include the "Recipients", the "Sender", and the "Administrator".

- **Notification Message –** Enter the text for the automated notification message.

## New Kaspersky Anti-Virus Controls

The following new options have been added to the **Mail Delivery → Anti-Virus** screen to allow greater flexibility in dealing with different types of results returned by the anti-virus scanner. These controls (enabled by default) allow the administrator to classify as a virus several types of attachments that may be unopenable, corrupt, password-protected, or cause scanning errors. It is strongly recommended that these types of attachments be treated as if they contained viruses.

The following types of attachments can be treated as viruses:

- **Attachments resembling a known virus** – Some types of attachments may resemble a known virus pattern and could contain malicious code. It is strongly recommended that you treat attachments with code that resembles a known virus as if they contained a virus.

- **Attachments containing unknown viral code** – The anti-virus scanner can detect code that resembles the patterns of a virus. It is strongly recommended that you treat attachments containing suspected viral code as if they contained viruses.

- **Corrupt attachments** – Corrupted attachments may not be able to be processed by the anti-virus scanner and could contain viruses. It is strongly recommended that you treat corrupt attachments as if they contained viruses.

- **Password-protected attachments** – Attachments protected by a password cannot be opened by the anti-virus scanner and could contain viruses. It is strongly recommended that you treat attachments that cannot be opened as if they contained viruses.

- **Attachments causing scan errors** – Attachments that are causing errors while being scanned by the anti-virus scanner may contain viruses. It is strongly recommended that you treat attachments that cause scanning errors as if they contained viruses.

## Brightmail™ and Intercept Changes

Administrators now have the option of configuring an independent action for Brightmail if they are running Brightmail in conjunction with the Intercept Anti-Spam engine.

In the **Mail Delivery → Anti-Spam → Brightmail** menu, a new option called "Brightmail Mode" has replaced the "Use Brightmail Anti-Spam in Intercept" option. The following modes can be used:

- **Disabled** – Disable Brightmail. No messages will be scanned by the Brightmail engine.

- **Perform Brightmail Actions** – Enable Brightmail and specifically use the Brightmail actions instead of the Intercept actions.

*Brightmail will trigger first before Intercept if the Brightmail mode is "Perform Brightmail Actions" and the Brightmail action is not skipped based on the Brightmail skip threshold.*

- **Use in Intercept Spam Decision** – Enable Brightmail and allow the Brightmail spam classification to be used in the overall Intercept decision.

*When using the Heuristic 1 and 2 Intercept strategies, messages classified by Brightmail as spam now score as "Certainly Spam", with or without additional objective measures. Messages classified as Brightmail "Suspected" spam will score as "Probably Spam" or "Certainly Spam" if there is at least one objective score as well.*

## Brightmail 6.0.3 Patch 167

This release updates the Symantec Brightmail Anti-Spam engine 6.0.3 with patch 167 that increases efficiency and addresses an issue with temporary directory space.

## RAID Monitoring

A new "RAID Status" item has been added to the *Status and Utility* screen to monitor the RAID array for MXtreme systems. An e-mail will be sent to the administrator if there is any degradation in the RAID array, including drive failures and RAID rebuilding operations.

## Flush DNS Cache

The ability to flush the DNS cache has been added to the *Status and Utility* screen. Administrators can click the **Flush DNS Cache** button to clear any incorrect or outdated DNS entries from the cache. This may be required if you have recently made changes in your DNS environment and the old entries are still cached on MXtreme.

# Product Notes

The following sections describe modifications and enhancements to existing features in this release:

## Modifications to Intercept Decision Strategies

The following modifications have been made to the Intercept decision strategies:

- **Heuristic 1** – The *Heuristic 1* strategy has been modified to de-emphasize Token Analysis. *Heuristic 1* is identical to *Heuristic 2* except that a spam message identified by only Token Analysis will not be marked as "Certainly Spam" or "Probably Spam". For spam messages to be marked as either "Certainly Spam" or "Probably Spam", one or two objective triggers, in addition to Token Analysis, are required.

- **Heuristic 1 and 2 and Brightmail** – Messages classified by Brightmail as spam now score as "Certainly Spam" when using the *Heuristic 1* and *2* strategies, with or without additional objective measures. Messages classified as Brightmail "Suspected" spam will score as "Probably Spam" or "Certainly Spam" if there is at least one objective score as well.

## Spam Quarantine Expiry Options

The options for Spam Quarantine message expiry have been modified to allow the administrator to choose between two different methods of expiry:

- **Expire per settings** – The Spam Quarantine will expire messages based on the administrator's configured settings.

- **Expire only on disk full** – The Spam Quarantine will expire messages based on the disk space percentage configured by the administrator. The default is 90% which expires messages from the quarantine when the disk is 90% full. Valid values are between 10% and 90%.

## Attachment Content Scanner Engine Upgraded

The Attachment Content Scanner engine has been upgraded providing support for additional file types, performance improvements, and resolves several issues.

## LDAP Server Retries

This update provides MXtreme with a retry mechanism for LDAP operations after an initial connection has been dropped by the LDAP server due to a period of inactivity. This causes subsequent LDAP lookups to fail. After the initial connection was dropped, subsequent LDAP lookups were failing. MXtreme will now attempt to connect to an LDAP server up to five times at 50ms intervals before timing out and returning an error. Retries will not be attempted if the connection fails because of issues with login credentials.

## F5 Version 9.2.x Support

MXtreme's F5 integration now supports F5 device versions 9.2.x.

## McAfee Anti-Virus Engine Update

The McAfee Anti-Virus option has been upgraded to version 5.0.00.

## Very Malformed Mail Moved

The *Very Malformed* configuration has been moved from the advanced section of the **Mail Delivery → Delivery Settings** screen to the main **Delivery Settings** screen.

## SQL Logging Removed

The SQL logging feature has been removed from the product.

## Null Character Detect in Attachments Removed

The *Enable NULL character detect* feature in **Mail Delivery → Content Management → Malformed Mail** has been modified to only look for null characters in the raw e-mail message and not attachments.

# Issues Fixed In This Release

The following issues are fixed in this release:

- The Attachment Control scanner failed to extract text from an AutoCAD `.dwg` file inside of a `.zip` archive.
- The Token Analysis feature was not training on messages that resulted in the Intercept action "Just Log".
- Brightmail rule set files were not being properly removed causing the number of disk inodes in a partition to fill up.
- Certain SPF macros were not being handled correctly.
- LDAP recipient checks were being performed before a virtual mapping was mapped. If the mapped recipient address did not exist, the message was not rejected.
- Dictionary files were not properly replicated to members in a cluster. Although the dictionary name appears on the member, the file's contents were not updated.
- After applying Update 1, the Spam Quarantine automatic expiry was not working.
- An issue with the Kaspersky Anti-Virus scanner and temporary files not being properly removed has been fixed.
- Additional backup processes were being created if a backup operation stalled eventually causing too many backup processes to be running at the same time.
- In some cases, the Disk Load Graph Report may contain no data for system hard disks.
- In certain cases, log indexing was not working properly.
- Threat Prevention list uploads to a Cisco device were not working.
- The time zone information for Sri Lanka has been updated.
- Threat Prevention would not process new requests when the IP address of a current request was simultaneously being removed from a data group due to the maximum number of entries for that group was exceeded.
- The "Maximum Message Size" value in **Mail Delivery → Mail Access** was not replicated to members in a cluster.
- In some cases, the DomainKeys signing feature was not properly deriving the organization domain name for a sender.
- When a base evaluation license expires or when a Specific Access Pattern reject is triggered, an incorrect error was returned followed by "554 Error: no valid recipients".
- A message with a RCPT TO: <@> would cause MXtreme to stop processing mail. Note that if messages with this issue still exist in the queue after installing Update 3, these messages must be removed or the problem will persist until they have all been removed from the queue.

- The SNMP Agent setting in the Network settings page was being replicated to members in a cluster.
- If a message with multiple recipients was rejected by the DNSBL feature, the sending server received a reject message for the first recipient, but the message was still delivered to the other recipients.

## Known Issues In This Release

The following are known issues in this release:

- If the PostX evaluation license expires, messages that cannot be encrypted are deferred and will not be delivered unless a new license is applied.
- If an invalid key server, port, or proxy server is defined in the PostX configuration, or PostX returns an error when trying to encrypt a message, the messages will be deferred and not delivered until the error condition is fixed. Error messages will appear in the mail logs when this occurs.
- PostX token files are not backed up and must be reapplied if an MXtreme is restored from backup. Token files are also not replicated to other members of a Cluster, and must be applied manually for each member.
- Changes made to a Threat Prevention Static List will not take effect until you click the **Apply** button in the main **Mail Delivery** → **Threat Prevention** screen.
- Any MXtreme 6.0 systems that were upgraded from pre-5.0 software may contain default PBMF filters that cause mail to be blocked. Administrators should remove all default BorderWare filters, or specifically delete PBMF filter 127 (`From,matches, "Resposta automática" webmaster@pib.com.br,accept`).
- When choosing a key size other than 512 for DomainKeys key generation, the interface will generate the keys and then revert the key size field to 512 when completed. This does not affect the key size chosen when the keys were originally generated.

# Dependencies

This update is for the MXtreme Mail Firewall version 6.0 only.

This release includes the previously released Update 1 and Update 2. If you have already installed Update 1 and/or Update 2, Update 3 can be installed on top of these updates.

⚠ *To uninstall these patches if they were already installed, Update 3 must be uninstalled first before uninstalling Update 1 or Update 2.*

# Installation Notes

This update release consists of the following file:

```
mx60_update_3.pf
```

It is strongly recommended that all users save a copy of the current configuration and backup MXtreme before proceeding with the upgrade. See the ***Backup and Restore*** section of the ***MXtreme User Guide*** for more detailed information on backing up and restoring the system.

**Installing the Update Software**
Update your MXtreme as follows:

1. Create a backup of your system via **Management → Backup & Restore**.
2. Select **Management → Software Updates**.
3. If you use Security Connection, the update will already appear in the *Available Updates* window and you can proceed to step 6.
4. If you are updating manually, click the **Browse** button in the *Upload Software Update* window and navigate to where you stored the `mx60_update_3.pf` file on your local system.
5. Click **Upload** to upload the file.
6. The update will now appear in the *Available Updates* window. Select the update file, and click **Install**.
7. Reboot the system.
8. The update will now appear in the *Installed Updates* window in **Management → Software Updates**.

**Updating MXtreme Systems in a HALO Cluster**
If you are applying this update to systems in a HALO cluster, you must update your Cluster Members first before updating the Cluster Console.

Update the Cluster Member systems as follows:

1. Create a backup of the Cluster Member system via **Management → Backup & Restore**.
2. On the Cluster Member, disable clustering via **Basic Config → Network**.
3. Perform the software update using the instructions in the ***Installing the Update*** section.
4. Reboot the Cluster Member.
5. Repeat the procedure on any other Cluster Members before updating the Cluster Console.

Update the Cluster Console as follows:

1. Ensure all Cluster Members have Clustering disabled.
2. Create a backup of your system via **Management** → **Backup & Restore**.
3. On the Cluster Console, disable Clustering via **Basic Config** → **Network**.
4. Perform the software update using the instructions in the ***Installing the Update*** section.
5. Reboot the Cluster Console.
6. When the Cluster Console has rebooted, enable Clustering via **Basic Config** → **Network**.
7. Enable Clustering on the Cluster Members via **Basic Config** → **Network**.
8. Recreate the cluster by adding the Cluster Member systems.

# Appendix A – Update 2 Notes

## New Features in Update 2

**URL Block Lists**
URL Block Lists contain a list of domains and IP addresses of web addresses that have appeared previously in spam, phishing, or other malicious messages. This feature is used to determine if the message is spam by examining any URLs contained in the body of a message to see if they appear on a block list. Similar to DNS Block Lists, the URL Block List will be queried to see if a URL exists on the configured block list server. If the sender is found to be on a Block List, then this information will be used by the Intercept engine to decide whether a message is spam or legitimate mail. If a URL matches on more than one URL block list, this will increase the weight of the score assigned by Intercept.

URLs can be checked by one of two methods:

- A SURBL (Spam URI Realtime Block Lists) method that performs lookups for a domain using the base domain or IP addresses of the URL. This is the default method.

- A DNSBL check that queries a DNS Block List server to lookup the full domain using the resolved host IP address for the URLs in a message.

BorderWare provides a default SURBL server that can be used for the URL Block List. Other SURBL or DNSBL lists can be added by the administrator, but caution must be taken when adding servers as some free services may introduce false positives.

URL Block Lists are configured via **Mail Delivery → Anti-Spam → Intercept → URL Block List**.

**Message Archiving**
This release adds archiving support to MXtreme allowing organizations to define additional mail handling controls for inbound and outbound mail. This feature is especially important for organizations that must archive certain types of mail for regulatory compliance or for corporate security policies.

MXtreme now allows mail to be categorized and selectively archived for different levels of importance. By providing the ability to classify and archive messages at different levels, mail of high importance or compliancy classification can be archived while allowing different actions for mail of lower importance. These features also prevent the waste of unnecessary resources by ignoring spam messages and other types of unwanted mail when archiving messages.

MXtreme can integrate with third-party archiving servers and archive e-mail messages by creating pattern filters to classify messages and route them to the appropriate archiving server or an archive e-mail address, while still delivering the e-mail to its original recipients. Mail headers added to an archived message by MXtreme allow administrators to customize their archiving services for efficient retrieval of archived messages.

Archiving can be used with Pattern Based Message Filters, the Objectionable Content Filter, and Attachment Content scanning, including the use of these features via Policies.

Archiving is configured via **Mail Delivery → Archiving**.

### New Anti-Spam Actions

The "Discard Mail" option (that rejects a mail message without notification to the sender) and the "Quarantine" option (to send the mail to the administrative quarantine area) have been added as possible actions for all Intercept Anti-Spam selections.

### Token Analysis Enhancements

The Token Analysis engine has been improved with the follow features to increase the spam catch rate, prevent false positives, and provide improvements to performance:

- Improves and refines JavaScript detection in HTML messages. The presence of JavaScript can be an indicator of a spam message.
- Detects non-standard port numbers in URLs (such as: `http://example.com:1234`)
- Detects basic phishing scams by comparing the URL in a message to its actual link.
- Stylesheet parsing has been improved to ensure that tokens are properly extracted from the message contents and not obfuscated by the stylesheet contents.
- Detects invalid IP address octets in the Received headers of a message (such as `123.456.789.012`)
- The initial token set has been enlarged and improved to detect the latest variants of spam and prevent false positives.
- In the advanced configuration of Token Analysis, administrators can now select which Intercept features will be trained for spam.

### Brightmail Skip Threshold

Brightmail processing can now be skipped depending on how Intercept has already classified the message. This feature can increase performance by skipping processing for a message already classified as spam. For example, Brightmail can be configured to skip processing if messages have already been classified by Intercept as "Certainly Spam". This feature is configured via **Mail Delivery → Anti-Spam → Brightmail**.

*Intercept Anti-Spam features must be enabled to skip Brightmail processing.*

### BSN Whitelist For Mail Relays

Administrators can now whitelist friendly local networks or addresses of known mail servers in their environment that relay mail via MXtreme. These specific networks and servers can be added to the "relays" IP Address list in the Threat Prevention feature to ensure that reputation statistics for these addresses will not be uploaded to BSN. The feature is configured via a link on the **Mail Delivery → Anti-Spam → Intercept → BorderWare Security Network** screen.

## Update 2 Product Notes

The following improvements and modifications have been made to current MXtreme features:

- The *IP Reputation* option in Intercept has been renamed to *Mail Anomalies*.

- BSN (BorderWare Security Network) configuration has been moved from the Intercept *IP Reputation* menu to **Mail Delivery → Anti-Spam → Intercept → BorderWare Security Network**.

- The null character detection option in the Malformed Mail feature has been modified to allow the administrator to specify how to check for null characters. Options are: "disabled", "in raw email", and "in raw email and attachments". The null character detection feature may cause incompatibility with certain mail servers and decoded attachments, and it is recommended that this feature be disabled if issues occur.

- A "State" column has been added to the Domain, Group, and User Policy screens to show which policies are enabled or disabled.

- Group policy can now be disabled if they are not being used for Policies in your organization. This may help performance for organization's that have a large number of Directory Users and do not need to use Group Policy. Click the **Disable Group Policy** button in the Group Policy screen to disable this feature.

- DomainKeys signing can now be enabled or disabled globally via **Mail Delivery → Domain Keys Signing**. If enabled, the use of message signing must be configured via Policies.

- When an outbound message is signed by DomainKeys, the event now appears in the *Mail Transport* log.

- The administrative quarantine area can now be searched for compliancy violations that have been quarantined. The subject, message text, or file name that has failed the compliancy check will be appended to the "Compliancy" classification, such as "Compliancy:[message subject]"

## Issues Fixed In Update 2

The following issues are fixed in Update 2:

### General

- If a space was inserted in the serial number when licensing Kaspersky Anti-Virus, the system appeared licensed but anti-virus pattern updates failed.

- Strong authentication settings were not being applied for non-admin users after MXtreme was restarted.

- The Health Check service was sending very large log files when reporting on a system.

- MXtreme was rejecting mail returned from an encryption server if "Trusted Subnet" was disabled for that network.

- The Attachment Content scanner was not properly timing out when it could not process a file.

- The Attachment Control scanner was not properly recognizing certain attachment types resulting in these known attachments types being blocked.

- Disabling the Encrypt/Decrypt feature did not disable it when using the Objectionable Content Filter.

- When a message was rejected by the *Mail Mapping as Access Control* feature, the intended recipient was not logged.

- Virtual mappings were still being applied after they were deleted.

- The "Maximum Recipients Reject Code" setting was actually taking its value from the "Maximum Unknown Recipients Reject Code" setting.

- A message with a RCPT TO: <@> would cause MXtreme to stop processing mail. Note that if messages with this issue still exist in the queue after installing Update 2, these messages must be removed or the problem will persist until they have all been removed from the queue.

**Intercept and Anti-Spam**

- Sending an internal mail message (such as those generated by a daily backup) with Token Analysis enabled and the local training threshold set to 0 caused issues with the scanner.
- Token Analysis data was not being purged properly during a database rebuild.
- Token Analysis scanning was still being performed even when it was disabled, or there were no pattern filters configured to check for tokens within messages.
- The "Train" action was being applied when a message matched multiple pattern filters.
- If a PBMF was created using a "RCPT TO" field, its action overrode the *Reject On Unknown Recipients* feature. This type of PBMF will now only override this feature if the priority is set to "high".
- When a server is rejected because of a DNS Block List, the returned reason included details of the rejecting DNS Block List server.
- Messages could not be released from the user spam quarantine via the spam summary notification message when the user name contained special characters.
- Certain SPF TXT record responses were not being parsed properly.
- Issues with DomainKeys selector name field validation have been fixed.
- The DomainKeys selector configuration was not replicating properly in a clustered setup.
- Issues were encountered when the selector for a DomainKeys signing policy was set to "none".
- The "Strip Incoming DK headers" option for DomainKeys authentication and the "Remove Duplicate Headers" option for DomainKeys signing were not working.
- Queue file write errors were appearing in the logs when sending a message with malformed DomainKeys headers.
- Certain mail servers were returning a "DomainKey-Status: bad format" header when canonicalization was undefined during MXtreme signing.

**Reporting and Logs**

- When reports did not generate correctly, subsequent reports could not be generated until the system was rebooted.
- The "Top Pattern Based Message Filter" field in a report displayed incorrect actions or extraneous data for some patterns.
- Advanced log searches were timing out when there was too much data to display.

- Older log files and indexes were not being rolled over properly.
- The MXtreme logging service was using a large amount of resources when working with large amounts of existing log files.
- A filtered System History search only allowed one page of returned data to be accessed.

**Policies and LDAP**

- MXtreme was not creating a corresponding mirror account for an imported LDAP account if an attribute was base64 encoded.
- MXtreme was treating RCPT TO e-mail addresses as case-sensitive when processing mail for the user spam quarantine and LDAP mirrored accounts.
- Organizations with a very large number of LDAP users and groups encountered long boot times when MXtreme was started.
- The Policy name was missing from the PBMF title when editing pattern filters for a policy.
- Clustering database issues were encountered when importing LDAP user and group information in a cluster.

**Threat Prevention and BSN**

- Threat Prevention was not properly counting messages classified as spam.
- Adding an IP address to the Threat Prevention internal address list to whitelist a server from BSN checks required a stop and start of the mail system.
- Threat Prevention was still rejecting an IP address after it had been removed from the permanent blacklist.
- New custom IP/CIDR static lists created by the administrator were not being applied by Threat Prevention.
- Threat Prevention would not process new requests when the IP address of a current request was simultaneously being removed from a data group due to the maximum number of entries for that group was exceeded.
- BSN and DNSBL information was only logged for the first message if a client sent multiple messages in one connection.

# Appendix B – Update 1 Notes

## New Features Added In Update 1

### DomainKeys™ Outbound Message Signing

This release builds on the DomainKeys support implemented in MXtreme 6.0 by adding the ability to sign outbound messages for authentication via DomainKeys. MXtreme supports the use of the Policy engine when signing outgoing messages, allowing administrators to configure signing for only specific domains or users that have been configured for use with DomainKeys.

### New DomainKeys Inbound Header Options

New options for receiving DomainKeys signed messages have been added to the **Mail Delivery → Anti-Spam → Intercept → DomainKeys Authentication** menu.

*The Intercept name for this component has changed from "DomainKeys" to "DomainKeys Authentication" in Update 1.*

- **Strip incoming DK headers** – Removes *Authentication-Results:* headers attached to incoming messages. This option protects against spammers who add a forged DomainKeys header to the message.
- **Add Authentication Header** – Adds an *Authentication-Results:* header to incoming messages
- **Temporary DNS Error** – Consider the message as spam in the event a DNS error prevents a DomainKeys lookup for a sender's key.

### BSN Relay Checks

Relay checks have been added to the BorderWare Security Network (BSN) configuration (**Mail Delivery → Anti-Spam → Intercept → IP Reputation)** to allow the administrator to check the received headers of a message for previous relays. These relays are then also checked for their reputation via BSN.

- **Check Relays** – How many previous received headers to check with BSN. Use this field to specify how many relay points should be checked. Acceptable values are between 0 and ALL. Recommended values are 0, 1 or 2. The default is 0.

- **Exclude Relays** – How many received headers to exclude from BSN checks, starting from the earliest. For example, setting this value to 1 means that the first relay point will not be checked. Recommended values are 0 or 1. The default is 0.

*Some ISPs include the originating dial-up IP as the first relay point which can lead to legitimate mail being classified as spam by BSN.*

### BSN Reject Message

A new option has been added to the **Mail Delivery → Anti-Spam → Intercept → IP Reputation** menu to customize the reject message for BSN. Use "%s" to specify the IP address of the rejected sender, such as:

```
go to http://intercept.borderware.com/lookup?ip=%s
```

### DNS Name Server Ordering

DNS servers (configured via **Basic Config → Network**) can now be queried either in strict order as specified in the configuration, or by the fastest response. If "Strict Ordering" is selected, the DNS servers will be queried in the order they are configured. If the first DNS server is unavailable, the next server in the list will be queried. For "Favor Fastest" mode, MXtreme uses DNS caching to determine which of the configured DNS servers is sending the fastest response. This is the default mode which will provide the best performance in most cases.

### Enhanced Language Support

This release adds support for the display of the UTF-8 character set in Reports and the Mail History. The UTF-8 character set supports almost every language, including most Western languages, Chinese, and Japanese. This support also allows PBMF filters in languages utilizing the UTF-8 character set. Support for half-width Katakana Japanese characters (as part of ISO-2022-JP) has also been added.

### Malformed Mail Encoded Null Character Detect

A new option has been added to the **Mail Delivery → Content Management → Malformed Mail** menu to detect null characters in an encoded message. When enabled, MXtreme will decode the e-mail and check for null characters (a byte value of 0) in the decoded message, in addition to null character checks in the raw mail body of a message. This feature can only be enabled if null character detection is already enabled.

*The encoded null character detection feature may cause incompatibility with certain mail servers and should be disabled if issues occur.*

### Maximum Recipients Reject Code

A new option to customize the *Maximum Recipients Reject Code* has been added to the **Mail Delivery → Mail Access** menu. This option allows administrators to define other errors to return instead of the default "452 Error: too many recipients" error, such as permanently rejecting the connection (554).

### Brightmail™ 6.0.3

The Brightmail engine has been updated to version 6.0.3. This update includes the latest signature rules and performance enhancements utilizing the BrightSig3 signature matching technology and performance enhancements. This update also includes Brightmail patch 163 for 6.0.3 that resolves issues with the MIME parser and BrightSig2 filters.

## Issues Fixed In Update 1

The following issues were fixed in Update 1:

### Security

This update resolves the following security issues:

- Internal safety checks used to prevent illegal or malformed account names from being entered at the login screen can trigger a system error when a malformation is detected. This error condition introduces a theoretical security issue.

- Internal safety checks against buffer overflow attacks caused error messages to be displayed directly in the administrative web browser interface. This condition is not considered a security issue, but the error handling engine has been fixed to eliminate any concerns raised during security audits.

### General

- Unexpected behaviour was encountered when an anti-virus pattern file update was triggered when an update was already in progress.
- Clicking on a message that has been quarantined because it was malformed revealed no information in the "Summary of Contents" section.
- MXtreme was classifying lost connections as "Pending" in the logs.
- Links to quarantined messages in a spam quarantine e-mail digest were expiring prematurely.
- Message parts that contained no name or data were being classified by Attachment Control as "[invalid name]" and were blocked when the default attachment action was set to "Block".
- 8-bit characters in a message *envelope-from* field or message attachment could not be quarantined.
- When offloading files, an intermittent socket error occurred causing certain files to not be offloaded.
- Log files were not being offloaded unless the *Keep Uncompressed* option was configured.
- An issue where certain open relay tests detected an open relay when MXtreme has SPF enabled has been resolved.
- Issues were encountered when the LDAP *Dereference Aliases* option was set to "Always".
- Issues with large Health Check service log files and entry validation have been fixed.

### PBMF (Pattern Based Message Filters)

- When selecting the PBMF link on the Policy screen, the current policy settings were not saved.
- The PBMF "Bypass" action was not bypassing BSN, DNSBL, and the Reject on Unknown Recipient features.
- When modifying a PBMF to use the "Reject", "Accept", or "Relay" action, the "Train" action would also be added, such as "Reject+train".
- The custom PBMF action "redirect" was not working when using certain message parts.
- PBMF filters using certain message parts are not following expected priority rules.
- The PBMF BCC action was not triggered when a "Bypass" action was taken.

### BSN and Threat Prevention

- Statistics uploads to the BSN network were not occurring unless the Threat Prevention feature was enabled.

- BSN stopped uploading new data to the BSN network after a certain period of time.
- When a dynamic list was removed from Threat Prevention, the accompanying entries were not removed from the connection rules script.
- Various reports were not correctly interpreting BSN statistics.
- BSN and DNSBL rejects were only being applied for the first recipient in a message and not the other recipients.
- Several issues with the mechanism for counting spam and clean messages for BSN statistics have been resolved.

### Intercept and Anti-Spam

- The DomainKeys weighting in the Intercept advanced settings was also being used as the weighting for SPF.
- E-mail messages with a large number of attachments caused scanning engine latency.
- Certain types of addresses in the RCPT TO part of a message (such as: `rcpt to:"\"User1\" <user1"@example.com>`), were not handled properly by the Brightmail engine.
- Anti-spam headers were not being added for messages without a body.
- The BCC function was still triggering for messages with an Intercept final action of "Reject".
- The Activity Screen showed "Pending" instead of "Rejected" for a message that was rejected by the Reject on Unknown Recipients feature.
- The Reject on Unknown Recipients feature was being bypassed if the local part of an e-mail address matched a local account on MXtreme.
- DNSBL relay checks were not working if the hostname included numeric characters.

### Policy and LDAP

- The group policy screen became slow and unresponsive when managing a very large number of users with multiple group memberships.
- Organizations with a very large number of LDAP users and groups encountered long boot times when MXtreme was started.
- Global low priority PBMFs were not being triggered when a Policy was triggered for a user.

# Appendix C – Message Processing Order

The following list describes the order in which incoming messages are processed by MXtreme with Update 3 installed:

**SMTP Connection Checks**

- Reject on Threat Prevention
- Reject on unauth SMTP pipelining
- Reject on expired MXtreme license
- Reject on Specific Access Pattern (SAP) HELO
- Reject on Specific Access Pattern (SAP) Envelope-To
- Reject on Specific Access Pattern (SAP) Envelope-From
- Reject on Specific Access Pattern (SAP) Client IP
- Reject on DNS Block List (DNSBL)
- Reject on BorderWare Security Network (BSN) reputation
- Reject on BorderWare Security Network (BSN) infected
- Reject on BorderWare Security Network (BSN) dial-up

At this point, local and trusted networks skip any remaining "Reject" checks.

- Reject on unknown sender domain
- Reject on missing reverse DNS
- Reject on missing sender MX
- Reject on non-FQDN sender
- Reject on unknown recipient
- Reject on missing addresses
- Reject if number of recipients exceeds maximum
- Reject if message size exceeds maximum

**Message Checks**

- Very Malformed
- Anti-Virus
- Pattern Based Message Filter (PBMF) Bypass (This action skips remaining checks)
- Malformed messages
- Attachment Control
- Threat Outbreak Control

*If the message is Malformed with the Malformed action of "Reject" or "Discard", Threat Outbreak Control will quarantine the message (if the action is set to "Quarantine"). The final action will be Threat Outbreak Control and "Quarantine" because of a possible virus.*

*If Attachment Control triggers with an action of "Reject" or "Discard", Threat Outbreak Control will quarantine the message (if the action is set to "Quarantine"). The final action will be Threat Outbreak Control and "Quarantine" because of a possible virus.*

- Message Affirmation
- Objectionable Content Filter (OCF)
- Pattern Based Message Filter (PBMF) (High priority)
- Pattern Based Message Filter (PBMF) (Medium priority)
- Trusted Senders List (Skips remaining checks)
- Pattern Based Message Filter (PBMF) (Low priority)
- Attachment Content Scanning
- SAP (Trusted and Allow)
- PostX Encryption (Trusted Only)

- Trusted Network (Skips remaining checks)

### Anti-Spam

- Brightmail Phase 1 (Only triggers if the Brightmail mode is set to "Perform Brightmail Actions". The Brightmail action is taken if Brightmail is not skipped and the message is Brightmail "Spam" or Brightmail "Suspected spam".)

- Intercept Anti-Spam Processing:

    - SPF
    - DomainKeys
    - Bulk Analysis
    - DNSBL
    - Message Anomalies
    - Spam Words
    - BSN Reputation
    - BSN Dial-up
    - Token Analysis
    - Brightmail (may be skipped and may not be included in Intercept)
    - URL Block lists

- Brightmail Phase 2 (Only triggers if the Brightmail mode is "Perform Brightmail Actions".)

### Message Mappings and Routing

- Mail Mappings
- Virtual Mappings
- Relocated Users
- Mail Aliases
- Mail Routing
- Mail Delivery to its final destination